511,249

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 October 2003 (23.10.2003)

PCT

(10) International Publication Number
WO 03/088663 A1

(51) International Patent Classification⁷: H04N 7/16, 5/00

(21) International Application Number: PCT/EP03/03856

(22) International Filing Date: 14 April 2003 (14.04.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
102 16 384.7 12 April 2002 (12.04.2002) DE

(71) Applicant (*for all designated States except US*): SCM MICROSYSTEMS GMBH [DE/DE]; Oskar-Messter-Strasse 13, 85737 Ismaning (DE).

(72) Inventor; and
(75) Inventor/Applicant (*for US only*): GENEVOIS, Christophe [FR/FR]; 34, avenue Marx Dormoy, F-83740 La Cadière d'Azur (FR).

(74) Agent: DEGWERT, Hartmut; Prinz & Partner GbR, Manzingerweg 7, 81241 München (DE).

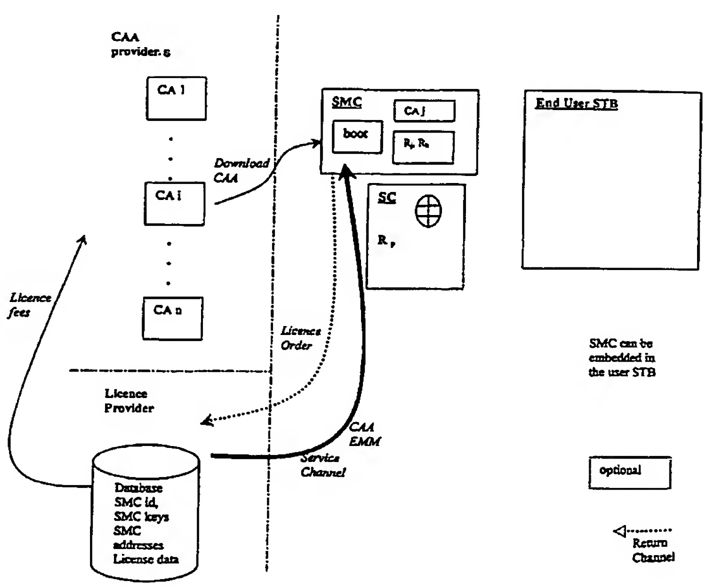
(81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: CONDITIONAL ACCESS NETWORK



(57) Abstract: In a conditional access network a provider distributes valuable contents such as digital TV over the network and end-users are allowed to access such valuable contents in function of individual access rights defined by a user license. The valuable contents are made available to the end-users by way of a plurality of different conditional access systems, each end-user is provided with a generic conditional access component having a basic functionality common to all conditional access systems, and particular conditional access systems are selectively enabled on each conditional access component subject to a successful verification of a corresponding license.

WO 03/088663 A1

Conditional Access Network

The present invention relates to a method of operating a conditional access network wherein a provider distributes valuable contents over the network and end-users are allowed to access such valuable contents in function of individual access rights defined by a user license. The invention also relates to a conditional access component for use in a conditional access network wherein a provider distributes valuable contents over the network and end-users are allowed to access such valuable contents in function of individual access rights defined by a user license.

In a conventional network for the distribution of valuable contents such as Digital Video Broadcast "DVB", the end-user is provided with a conditional access unit that is either embedded in a Set-Top-Box or constitutes a pluggable module for insertion into a Common Interface ("CI") slot of a Set-Top-Box. In either case, the conditional access unit includes a SmartCard reader for accommodation of a subscriber card, i.e. a SmartCard (a Chip card) that contains required functionality and data to control secured access to the valuable contents in conjunction with the conditional access unit.

Due to general aspects of security, such as the level of protection against intrusion, and to technical requirements such as data formats, video resolution etc., content providers use different conditional access systems, and each conditional access system requires a specific conditional access component which the end-user must acquire to gain access to contents distributed with that particular conditional access system. A conditional access component includes both hardware and software, the software including a content provider's

application. At the time of manufacture, the application is loaded into the non-volatile memory of the component, and a license fee is usually paid by the manufacturer to the content provider. The purchase price for a particular conditional access component thus includes a license fee.

The present invention provides a new way to allow an end-user to gain access to valuable contents distributed in any of a plurality of conditional access systems with just one conditional access component that has a basic functionality common to all of the plurality of conditional access systems, and that can be selectively enabled for any of the plurality of conditional access systems subject to the successful acquisition of a license. Thus, the invention allows an end-user to be authorized in consuming services from several different CA systems with the same device (contrary to the current state of the art where the device is linked to the CA). This device is then able to host one or more CA applications and one or more related authorizations, at the same time.

According to the invention, a method of operating a conditional access network is provided. Providers distribute valuable contents over the network and end-users are allowed to access such valuable contents in function of individual access rights. The valuable contents are made available to the end-users by way of a plurality of different conditional access systems. End-users are provided with a generic conditional access component having a basic functionality common to all conditional access systems. Particular conditional access systems are loaded on the conditional access components. The particular conditional access systems thus loaded on the component are initially disabled. A license is acquired for a particular conditional access system and the conditional access system is enabled subject to a successful verification of the license.

The invention also provides a conditional access component for use with the method. Specifically, the invention provides a conditional access component for use in a conditional access network wherein providers distribute valuable contents over the network and end-users are allowed to access such valuable contents in function of individual access rights. The component has a basic functionality

common to a plurality of different conditional access systems used in the network. For each particular conditional access system to be used in the component, specific application software is loaded into a non-volatile memory of the component. A new application thus loaded is initially disabled. The component includes a license verifier. When a valid license for a particular conditional access system is found, the corresponding application is enabled.

Further features and advantages of the invention will become apparent from the following description with reference to the drawings. In the drawings:

- Figure 1 is an overall view illustrating the relationship between an end-user side equipment, a number of conditional access application providers and a license provider;

- Figure 2 is a block diagram illustrating a head-end conditional access application enabler framework;

- Figure 3 is a block diagram of a conditional access component;

- Figure 4 is a flowchart illustrating essential steps of a procedure enabling the conditional access component to access contents received in a transport stream under a particular conditional access system.

Glossary, definition of entities and data:

AACC	Authorized Automatic CA Configuration
ATR	Answer To Reset: data sent by a smart card when it is plugged in
CAAP	(CA application Provider) the entity that permits the secure download of CAA to the SMC.
CAA	(CA application: the code that runs within the SMC, giving access to the related CAS services.

CA_ID	Unique identifier of the CAS.
CAS	(CA system) a system that enables an end-user to access to payTV programs
CAT	CA Table, that contains the CAS descriptors (parameters, data, scripts ...).
End-user	The people that want to watch the tv and pay for that.
Firmware	all kind of binary code stored in the SMC (e.g. boot, OS, applications, drivers, ...)
Licence	This element allows the SMC to run legally the related CAA.
LO	(Licence Order) this procedure permits to an end-user to acquire from the LP the right to run a CAA, having then access to its payTV programs.
LP	(Licence Provider) this entity
LT	Licence Table, that contains the CA Licence descriptors (parameters, data, scripts, ..).
MMI	Man Machine Interface: a resource provided by the STB to the SMC to allow it to display data.
Subscription	
payTV programs	Programs scrambled under control of a specific CAS.
SC	(Service Channel) a channel that carries parameters (configuration file, data, scripts) related to each CAS
Script	a sequence of commands that are executed by the SMC
SerNo	Serial Number, unique value that identifies an entity (SmCa, SMC, ...)
SMC	Secure MultiCAS Component: It is made of one or more devices; is a secure one, able to store, run and/or handle applications & data in a secure way: it means that any element within is protected against modification and illegal access.
SmCa	Smart Card
SMC keys	secret and/or public data used for security-orineted services (e.g. integrity, authentication, confidentiality)
TS	Transport Stream

TiSe (Timing Service) a service that provides right date and time, available either outside or inside the SMC (e.g. a clock).

Sequence of operations:

1 the end-user buys the component (SMC)

2,in parallel:

2 he retrieves the CA Application that will run on the device

2' he acquires the authorization to use such application

3 he consumes the CA services

The steps 2 and 2' could be made in any order.

Description of the different actions to be considered :

1. SMC purchasing

   The end-user buys a SMC.

   This device does contain at least boot firmware, able to manage security, handle smart cards, perform secure download, process licences. The SMC could also embed some other applications such as CAA (one or more). In term of data, it could embed one or more licences for one or many CAS.

2. CAA Acquisition

   In this part, we develop the process used for acquiring the CA Application and the parameters needed to configure the CAS and the SMC.

   Conditional Access Application means the firmware needed to process the encrypted A/V data using the different keys and licence in order to deliver a clear content to the end-user according to its rigths.

   Three steps must be passed to get a CAA "pending" ready to be activated inside the SMC : CAA identification, CAA configuration and CAA acquisition.

CAS identification

1. The SMC retrieves CASs descriptors by listening the CAT on the SC (which is always available to the SMC).
2. identification is triggered by an event:

- it could be a manual event (through MMI):The user can access a menu proposing CASs available for the end-user.
- it could be one of the following four events:
    - SmCa insertion : If the user inserts a SmCa into the SMC, then a process of automatic CAS identification is launched.

- Module insertion or Module menu : the Module firmware can propose a set of CAAs that are identified as present and in the Service Channel, through the CAT.
- Content triggering, downstream event : If the channel selected by the user is protected by a CAS requiring a specific CAA not present as valid in the SMC, and if the considered CAA is conform to the AACC, then a new CAS is automatically identified.
- License presence (means step 2' has been already performed): If the license corresponding to a CAA is present and valid in the SMC, then the corresponding CAA is identified as required by the CAS to go on configuration phase.

At this step, the CAS has been choosen.

3. The SMC checks the presence of the corresponding CAA inside it.
4. If the considered CAA is present and conform to the latest version (using information coming from the CAT), then the CAA acquisition is considered as achieved.
5. If the considered CAA is not present or in an older version, then the CAS identification is complete.

At the end of the CAS identification, the SMC knows **CA_ID** and may have **CAA.**

CAA Configuration

Once identified, the CAA needs a lot of dynamic parameters to be set. The fact that different CASs can be loaded inside the SMC, added to a need of adaptation skill to prevent obsolecence of the architecture implies that the CAA could come with its parameters through a dedicated specific Service Channel.

The Service Channel can be a database carried by the downstream, and containing the following parameters that will allow

- the CAS to be configured and downloaded using for example a script.
- and the SMC itself to be configured to integrate the new CAA.

Some of the parameters can be used by both the CA and the SMC, and can be :

- the ATR of the SmCa in order to identify it
- The SerNo corresponding to the Smart Card or to the CA to be downloaded (including e.g. mask features for zoning)
- The script describing the method to be used to download the CAA firmware (location of data, files locations and their signature ...
- A reference to the license needed to unlock the CA.

At the end of the CAA configuration, the SMC knows **CA_ID and how and where it can get the latest version of the CAA.**

CAA acquisition

Once identified and configured, the CAA must be acquired by the SMC (e.g. by a download). At the end of this process, the CAA will be fully available to the system, but will remain locked until all the rights (especially the license) have been checked sucessfully.

The CAA acquisition can be proceeded as following :

1. The CAA can be already present in the SMC , whether because the system was sold with this CAA inside, or because this CAA was already acquired (pre-stored) in the system in a previous session. Then, its integrity and validity must be checked, and the acquisition is considered as ended.
2. The script contained in the Service channel can be ran in order to download the CAA over the air, setting the tuner on the appropriate transponder and channel, and filtering the downstream in order to collect the correct files.

At the end of the CAA acquisition, the SMC has **the latest version of the CAA relative to the CA_ID.** The CAA is in a locked state until the license and required rights have been checked as valid and up-to-date.

2'. Licence acquisition

2'0. Description of the licensing system

The CAA enabler Head End (owned by the LP) is :

- a CAA EMM builder,
- an encryption unit (ENC) and
- a database to store information like SMC identifier(SMC id), SMC addresses and SMC keys in a secure manner.

This Head End component will generate CAA EMMs (used for Licence transport) in MPEG packet format and sends these to the connected multiplex (MUX)that receives also Video/Audio data, standard EMM and ECM, Service Information (SI) and Program Service Information (PSI). In addition it transmits the CAA EMM Packet Identifier (PID) and the CA_SYS_ID to the SI/PSI generator.

The task of the SI/PSI generator is to modify the Conditional Access Table(CAT), i.e. to add a ca_descriptor() containing the CAA EMM PID and the CA_SYS_ID. The purpose is to signal the CAS where it will find the CAA EMM stream. The mechanism is identical to the one used for the EMM play out.

On the receiver side, in the SMC, the CAA enabler consists of three components:

· the CAA EMM filter,

· the verifier (a part of the firmware that is able to check EMM validity) and

· a secure storage to store SMC SerNo, SMC addresses, SMC keys and control data. This storage area is protected against unauthorized access and modification.

The CAA EMM filter extracts the CAT from the encrypted transport stream TS* and analyses it to get the PID where the CAA EMM stream is played out. The next task is to interpret the CAT to find the CAA EMM which is addressed to the specific module. If one is found the filter unit sends the CAA EMM to the verifier.

The verifier uses a SMC key to proof the authenticity of the EMM (e.g. by using digital signature feature) and in the case of a successful verification, it decrypts the CAA EMM. The next step is to process the instructions of the CAA EMM payload. In the case of an activation the SMC enables e.g. the de-scrambler to produce the clear stream TS.

2'.1 Licence Identification:

The end-user selects manually or automatically, thru the SMC, the CAS he wants to acquire. It leads for the SMC to the knowledge of the CA_ID.

It could be done in different manners:

2'.1.a insertion of the SMC, or service selection: it then triggers a select feature, thru an MMI, (e.g. using a menu and the remote control).

2'.1.b insertion of the CA smart card: it then identifies the CA_ID, as it is embedded in the smart card. This value is sent to the SMC.

2'.1.c content triggering: by choosing himself a channel or a service, the end-user selects and identifies the CAS.

At the end of this point, the SMC knows the **CA_ID**

2'.2 Licence Configuration

The SMC retrieves all parameters (e.g. fees, phone number, SerNo, licence options) associated to the CA_ID,required for Licence access, in order to perform the retrieval of the CA-licence. This information can be taken in the Service Channel (from the LT) or in a fixed database stored in the SMC.

At the end of this point, the SMC knows **where and how access to the CA licence(s).**

2'.3 Licence Acquisition:

If a return channel exists,

- the end-user processes a request to the LP for the CA-licence, to do that, the end-user, using config parameters, requests for a licence from the LP (e.g. financial transaction), bringing in the sent data everything requested by the LP (e.g. SMC SerNo, identity, ...).
- the LP sends the specific licence, after complete payment, the LP processes data specific to the end user SMC and the chosen CAA, and sends them to the SMC (e.g. EMM).

If no return channel exists

- the end user buys a prepaid card, embedding a CA-licence
- the licence is downloaded in the SMC, made specific (i.e. the licence is linked to the SMC SerNo).
- Later, when rights are used, the credits in the card are burned.

At the end of this point, the SMC has a **licence of use for a specific CAS.**

3. Consumption of PayTV programs

The end-user wants to consume programs or services. The CAA enabler feature requires some additional hardware resources on the head end component and on the SMC component. This is described in 2'0.
Here is the sequence :

3.1 the end user selects a channel or a service he wants to consume
3.2 the SMC checks the corresponding CAA (i.e. CAA(CA_ID(channel)):
(optional) checks presence of the smart card related to the CA
checks that the CAA is not corrupted and locked
3.3 the SMC checks the CA licence:
checks the licence presence
checks the licence parameters are OK (date-by using the TiSe-, identity, SerNo, ..).
3.4 the SMC runs the CAA.

Claims

1. A method of operating a conditional access network wherein providers distribute valuable contents over the network and end-users are allowed to access such valuable contents in function of individual access rights, characterized in that the valuable contents are made available to the end-users by way of a plurality of different conditional access systems, end-users are provided with a generic conditional access component having a basic functionality common to all conditional access systems, particular conditional access systems are loaded on the conditional access components, the particular conditional access systems thus loaded on the component are initially disabled, a license is acquired for a particular conditional access system and the conditional access system is enabled subject to a successful verification of the license.

2. The method of claim 1, wherein the valuable contents are distributed in a digital transport stream that contains Entitlement Management Messages "EMMs" specific to each conditional access system.

3. The method of claim 2, wherein each conditional access component includes a filter unit for filtering out the specific EMMs of conditional access systems enabled on the component and a verifier unit for the verification of access rights defined by the filtered specific EMMs.

4. The method of claim 3, wherein the valuable contents in the transport stream are scrambled, each conditional access component has a descrambler adapted to process a scrambled transport stream into a clear transport stream, and the descrambler is enabled or disabled in function of a successful or unsuccessful verification, respectively, of the access rights.

5. The method of any of claims 1 to 4, wherein each conditional access system has an associated application for execution by the conditional access component.

6. The method of claim 5, wherein applications are downloaded over the network from a conditional access application provider.

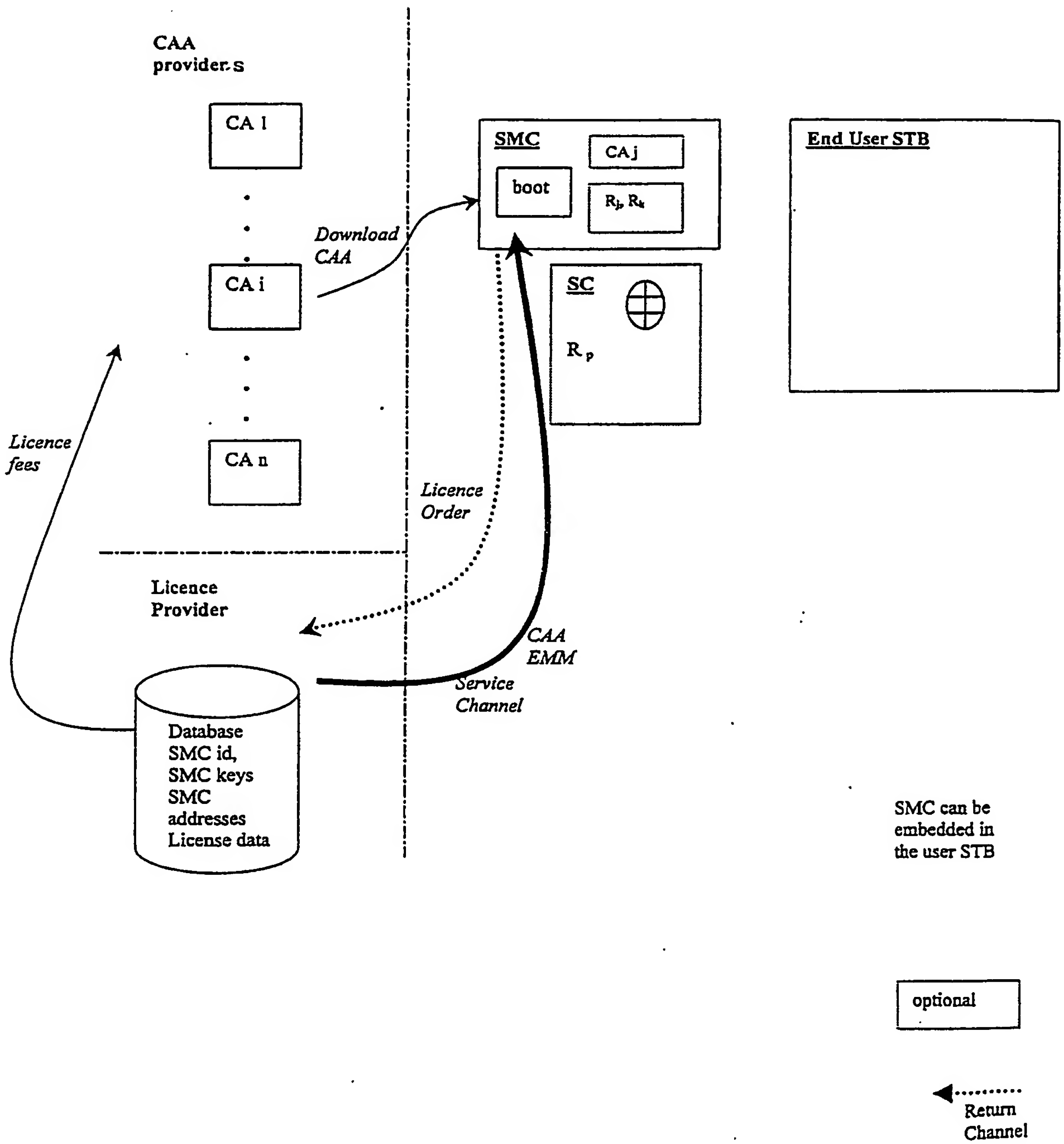
7. The method of any of claims 1 to 6, wherein the network includes service channels for the transmission of configuration data to the conditional access components.

8. A conditional access component for use in a conditional access network wherein a provider distributes valuable contents over the network and end-users are allowed to access such valuable contents in function of individual access rights defined by a user license, characterized by a basic functionality common to a plurality of different conditional access systems used in the network, a non-volatile memory for storing specific application software that constitutes a particular conditional access system in conjunction with the basic functionality, the particular conditional access system being initially disabled when the specific application is loaded in the non-volatile memory, means for acquiring a license for the particular conditional access system, and means for selectively enabling the particular conditional access system subject to a successful verification of a corresponding license.

9. The conditional access component of claim 8, comprising a memory for storing at least one conditional access application associated with a particular conditional access system and means for loading said application into said memory.

10. The conditional access component of claim 8 or claim 9, the valuable contents being distributed in a digital transport stream that contains Entitlement Management Messages "EMMs" specific to each conditional access system, and comprising a filter unit for filtering out specific EMMs of conditional access systems enabled on the component and a verifier unit for the verification of access rights defined by the filtered specific EMMs.

Fig.1



CAA
providers
CA 1
CA i
CA n
Download
CAA
Licence
fees
Licence
Provider
Database
SMC id,
SMC keys
SMC
addresses
License data
SMC
CA j
boot
R_j, R_k
SC
R_p
End User STB
Licence
Order
CAA
EMM
Service
Channel
SMC can be
embedded in
the user STB
optional
Return
Channel

Fig. 2

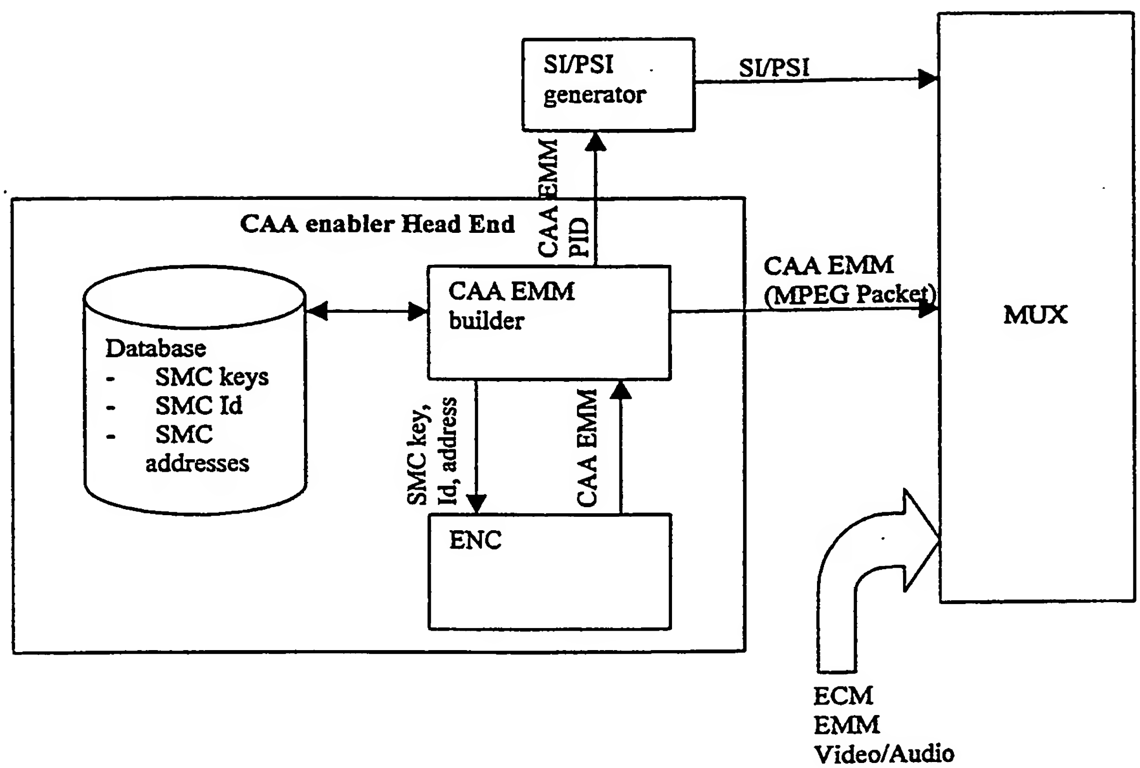

SI/PSI generator
SI/PSI
CAA enabler Head End
CAA EMM PID
Database
- SMC keys
- SMC Id
- SMC addresses
CAA EMM builder
CAA EMM (MPEG Packet)
MUX
SMC key, Id, address
CAA EMM
ENC
ECM
EMM
Video/Audio

Fig. 3

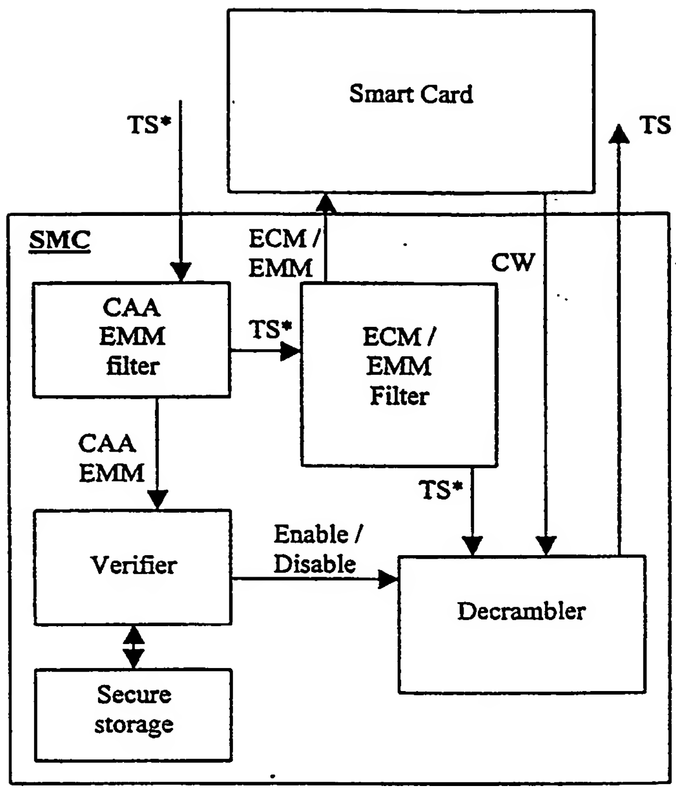
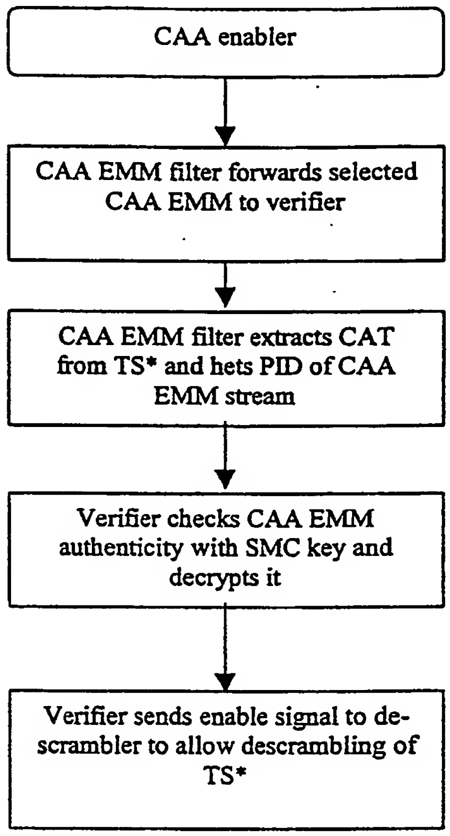

Smart Card
TS*
TS
SMC
ECM / EMM
CW
CAA EMM filter
TS*
ECM / EMM Filter
CAA EMM
TS*
Enable / Disable
Verifier
Decrambler
Secure storage

Fig. 4

Flow chart of CAA enabler on the SMC side



INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/03856

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/16 H04N5/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 0 964 573 A (THOMSON MULTIMEDIA SA) 15 December 1999 (1999-12-15) abstract page 2, line 22 -page 4, line 35; figures 3,4A ---	1-10
Y	EP 0 696 141 A (NOKIA TECHNOLOGY GMBH) 7 February 1996 (1996-02-07) abstract column 7, line 3 -column 7, line 54 column 10, line 9 -column 10, line 32 --- -/--	1-10

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 September 2003	18/09/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Schoeyer, M

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP 03/03856

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	EBU POJECT GROUP B/CA: "FUNCTIONAL MODEL OF A CONDITIONAL ACCESS SYSTEM" EBU REVIEW- TECHNICAL, EUROPEAN BROADCASTING UNION. BRUSSELS, BE, no. 266, 21 December 1995 (1995-12-21), pages 64-77, XP000559450 Grand-Saconnex, CH ISSN: 0251-0936 the whole document ---	1-10
Y	WO 96 08912 A (HARDING MICHAEL V ;NEWBY CHARLES F (US); TITAN INFORMATION SYSTEMS) 21 March 1996 (1996-03-21) page 5, line 13 -page 6, line 5; claims 32-45 page 11, line 16 -page 11, line 19 ---	1-10
A	WO 01 26372 A (THOMSON LICENSING SA ;DEISS MICHAEL SCOTT (US); DIASCORN JEAN LOUI) 12 April 2001 (2001-04-12) abstract ---	2,10
A	US 5 420 866 A (WASILEWSKI ANTHONY J) 30 May 1995 (1995-05-30) abstract; figure 7B -----	2,10

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP 03/03856

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0964573 A	15-12-1999	EP 0964573 A1	15-12-1999
		CN 1239375 A	22-12-1999
		EP 0964574 A1	15-12-1999
		JP 2000069451 A	03-03-2000
		KR 2000005735 A	25-01-2000
		US 6543050 B1	01-04-2003
		ZA 9903666 A	02-12-1999
EP 0696141 A	07-02-1996	FI 943582 A	02-02-1996
		DE 69512335 D1	28-10-1999
		DE 69512335 T2	06-04-2000
		EP 0696141 A2	07-02-1996
WO 9608912 A	21-03-1996	AU 4461996 A	29-03-1996
		CA 2199526 A1	21-03-1996
		DE 69525170 D1	14-03-2002
		DE 69525170 T2	10-10-2002
		EP 0787391 A1	06-08-1997
		ES 2171568 T3	16-09-2002
		WO 9608912 A2	21-03-1996
		US 6115821 A	05-09-2000
		US 6108422 A	22-08-2000
		US 5796829 A	18-08-1998
WO 0126372 A	12-04-2001	AU 7998500 A	10-05-2001
		BR 0014511 A	11-06-2002
		CN 1378742 T	06-11-2002
		EP 1226717 A1	31-07-2002
		JP 2003511917 T	25-03-2003
		WO 0126372 A1	12-04-2001
US 5420866 A	30-05-1995	AU 687844 B2	05-03-1998
		AU 7220994 A	17-10-1995
		CA 2186368 A1	05-10-1995
		JP 2940639 B2	25-08-1999
		JP 9511369 T	11-11-1997
		WO 9526597 A1	05-10-1995